Tenda®
腾达网络 以人为本

型号:W330R

用户手册

www.tenda.com.cn



Wireless-N 宽带路由器

版 权 申 明

目录

第1章： 产品介绍

感谢您购买 W330R Wireless-N 宽带路由器（以下简称路由器）。W330R 采用高级 MIMO（多进多出）技术，基于 IEEE802.11n（draft 2.0）标准，扩展无线网络的覆盖范围，并提供最高 300Mbps 的稳定传输，且向下兼容 IEEE802.11b/g。该设备集路由器、无线接入点、四口千兆交换机、防火墙于一体，适用于个人用户、小型办公室、小型企业等。独有的“一键设定”智能软件使安装更简便。

W330R 支持 WDS 功能（无线分布式系统），用以实现信号的中继和放大，从而延伸无线网络的覆盖范围；支持“一键加密”功能，使您无须再记录烦琐的密码；支持手动关闭 SSID 广播、端口过滤以及 MAC 地址过滤规则,保护您的网络远离恶意侵入。

Web 管理接口可以方便您使用浏览器通过本地局域网登陆进行管理，支持远程 WEB 管理，用户无论在何地，都可以通过 Internet 轻松管理路由器；真正支持 WMM，让您的语音视频更流畅。

物品清单

- W330R 无线宽带路由器一台
- 以太网网线一根
- 快速安装指南一张
- 电源适配器一个
- 光盘一张
- 保修卡一张

如果上述配件有损坏或短缺，请您及时和产品经销商联系。

第 2 章： 认识 Wireless-N 宽带路由器

后面板接口说明及图示

后面板图示：



后面板接口说明：

后面板接口	说　明
LAN(1-4)	连接至计算机的以太网网卡，也可级联至集线器或交换机
RESET	**注意!!!** 当您按住此键 7 秒后，您设定的资料将被删除，并恢复出厂设置
WAN	连接 ADSL 或是 CABLE MODEM、小区宽带
DC IN	DC12V/1 A 电源插孔

前面板图示及说明

在 W330R 的前面板上有 LED 的显示灯。显示如下图：



注意：

本产品的有线端口（1 个WAN口和 4 个LAN口）是10/100/1000Mbps端口，当端口工作在 1000Mbps模式下LED指示灯为绿色，工作在 10/100Mbps模式下LED指示灯为红色。

指示灯	状态	描述
POWER	常亮	表示电源供电正常
SYS	闪烁	表示系统运行正常
WAN	常亮	表示 WAN 口连接正常
	闪烁	表示路由器 WAN 口正在进行数据传输
WLAN	闪烁	表示无线信号正常
LAN(1/2/3/4)	常亮	表示 LAN 口连接正常

	闪烁	表示路由器 LAN 口正在进行数据传输
WPS	闪烁	表示路由器在 WPS 模式下正在与客户端进行认证协商

硬件安装

在设置路由器之前，请您按照如下步骤进行正确连接。为了保证更好发挥路由器的无线性能，请把路由器置于覆盖区域中间位置。

1、请使用网线将路由器 LAN 口与您的计算机网卡连接。	
2、请使用标配的电源适配器给路由器供电。	
3、将您的宽带线（电信 ADSL、网通 ADSL、长城宽带、天威视讯等）与路由器的 WAN 口连接。	

注意：

请使用附带的电源适配器。使用不相同的电源适配器可能会对路由器造成损坏。

第3章： 连接到宽带路由器

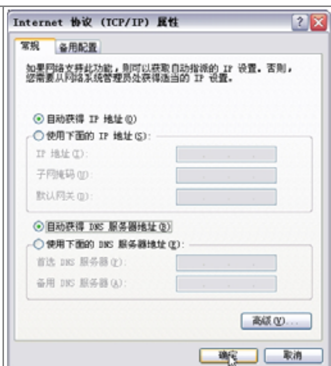
为了快速正确地完成路由器设置，请您参照以下步骤进行设置。

正确设置您的计算机网络配置

1、在您正在使用的桌面上，用右键单击“**网上邻居**”，在弹出的菜单中选择“属性”	
2、在随后打开的窗口里，用鼠标右键点击“**本地连接**”，选择“**属性**”；	
3、在弹出的对话框里，先选择“**Internet 协议（TCP/IP）**”，再用鼠标点击“**属性**”按钮；	

4、在随后打开的窗口里，您可以选择“**自动获得 IP 地址（O）**”或者是“**使用下面的 IP 地址（S）**”；

a、“**自动获得 IP 地址（O）**”如图：



b、“**使用下面的 IP 地址（S）**”

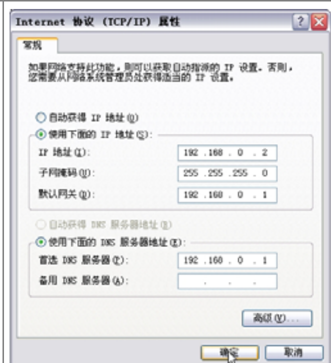
IP 地址：192.168.0.XXX：(XXX 为 2~254)

子网掩码： 255.255.255.0

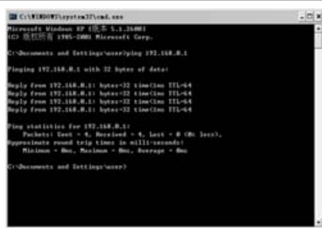
网关:192.168.0.1

DNS 服务器：您可以填写您当地的 DNS 服务器地址（可咨询您的 ISP 供应商）也可以由路由器作为 DNS 代理服务器。

设置完成后点击“**确定**”提交设置，再在本地连接“**属性**”中点击“**确定**”保存设置。



验证网络正常连接

1、选择“**开始—>所有程序—>附件—>命令提示符”**；	
2、按右图格式输入“**ping 192.168.0.1**”并回车，如能得到图示的回应，则表明您的计算机与路由器连接正常。	

登陆路由器

1、打开 Web 浏览器，在地址栏中键入"**http：//192.168.0.1"**，并回车。	地址(D) http://192.168.0.1/
2.在弹出登陆窗口中,输入用户名:**admin,** 密码:**admin,**然后单击 “确定”	连接到 192.168.0.1 300M Wireless-N Broadband Router 用户名(U): admin 密码(P): ***** 记住我的密码(R) 确定 取消
3、如果您输入的用户名和密码正确，浏览器将进入管理员模式的画面。	

第4章： 基本配置

这部分主要向您介绍如何通过 WEB 页面完成基本的路由器设置。

设置向导

本向导可以帮助您快速设置路由器的工作模式及基本参数。单击“**下一步**”。	
出现右图所示页面，此路由器支持三种常用上网方式（**ADSL 虚拟拨号，动态 IP，静态 IP**），请根据自己使用的实际情况进行选择，如果您对 ISP 接入方式不清楚时，可以启用自动检测功能来完确定您的接入方式。选择相应的接入方式后，请单击“**下一步**”。	

➔**连接模式 1：** ADSL 虚拟拨号(PPPoE)请输入网络服务商提供给您上网帐号及口令。如您遗忘或不太清楚，请咨询您的网络服务商。

例如：

上网账号	sztenda@163.gd
上网密码	123456

➔**连接模式 2：** 动态 IP (DHCP)

如果网络提供商提供给您的接入方式为动态 IP（意味着您每次连接时可能获取到不同的 IP 地址），请选择“**以太网宽带，自动从网络服务商获取 IP 地址（动态 IP）**”，您不需要像其它二种模式需输入相关上网参数，点击“**下一步**”，然后点击“**保存**”即可。

➔**连接模式 3:**静态 IP

如果网络提供商提供给您的接入方式为静态 IP，请选择“**以太网宽带，网络服务商提供的固定 IP 地址（静态 IP）**”您需要把 ISP 或网络管理员提供给您 IP 地址，子网掩码，网关，DNS 服务器，备用 DNS 服务器填入到相关选项。

例如：ISP 提供给您的：

IP 地址	192.168.1.2
子网掩码	255.255.255.0
网关	192.168.1.1
DNS 服务器	202.96.134.133
备用 DNS 服务器	202.96.128.68

那么您需如图填入相关参数信息。

完成后请点击“**保存**”按钮完成设置，系统将记录您所填写的参数；为保证设置生效，建议您在左边的功能菜单“系统工具”中选择“重启路由器”，使路由器使用新的参数运行。	
路由器重启完成后，您可以点击右边菜单的“**运行状态**”，查看路由器与 ISP 局端的连接状况。WAN 口出现如图所示的状态信息，恭喜您，已经完成路由器基本上网设置，现在可以上网冲浪了。如果需要进一步设置更多的功能，请参考下一章节的内容。	

第 5 章： 高级设置

本章节指导您完成路由器高级配置，包括 LAN 口设置，WAN 口设置，MAC 地址克隆和 DNS 设置。

LAN 口设置

本设置页面介绍路由器 LAN 口相关参数的配置。 **MAC 地址**：显示本路由器对局域网的 MAC 地址，此值不可更改。 **IP 地址**：本路由器对局域网的 IP 地址。该地址出厂设置为 192.168.0.1，您可以根据需要改变它。 例如：把路由器的 IP 地址更改为:192.168.3.1，如图 ***注意：*** **如果您改变了本IP地址，您在下次登录路由器时必须使用新的IP地址才能进入WEB**	LAN口设置 本页设置LAN口的基本网络参数。 MAC 地址 00:13:45:60:14:50 IP地址 192.168.3.1 子网掩码 255.255.255.0 保存 还原

管理界面，而且，您局域网内的所有计算机的默认网关必须设置为该IP地址才能正常上网。 **子网掩码：**本路由器对局域网的子网掩码，默认设置为255.255.255.0。	

WAN 设置—虚拟拨号（PPPoE）

WAN 口连接类型：显示当前选择使用的模式。 **上网账号：**输入网络服务商（ISP）提供给您的上网账号。 **上网口令：**输入网络服务商（ISP）提供给您的上网口令。 **MTU：**最大传输单元(Maximum Transmission Unit)。默认值为 1492。若	

非必要，请不要改变默认数值。 **服务名：**指当前设置PPPOE 的连接名称，如非必要，请勿填写。 **服务器名称：**服务器名称，如非必要，请勿填写。 **自动连接：**在开机或断线后自动连接。 **手动连接：**当网络连接断开后，由用户手动进行连接。 **按需连接：**在有数据访问时自动进行连接。 **定时连接：**在指定的时段自动进行连接。 ***注意：*** **只有当您到“系统工具”菜单的“时间设置”项设置了当前时间后，“定时连接”功能才能生效。**	

WAN 口设置—静态 IP

如果您的模式选择为静态 IP，则在按图示输入相关参数信息。

IP 地址：请您输入 ISP 提供给您的 IP 地址，此地址是路由器对广域网的地址。如有不清楚，可以咨询您当地的网络服务商。

子网掩码：请您输入 ISP 提供给您的子网掩码，此掩码是路由器对外网的子网掩码,一般值为 255.255.255.0

网关：请您输入 ISP 提供给您的网关，如有不清楚可以咨询当地的网络服务商。

主 DNS 服务器：请您输入 ISP 提供给您的主 DNS 服务器地址。

备用 DNS 服务器：请您输入 ISP 提供给您的备用 DNS 服务器地址，该项可选。

WAN口设置

WAN口连接类型： 静态IP

IP地址 192.168.100.115

子网掩码 255.255.255.0

网关 192.168.100.100

DNS服务器 192.168.100.205

备用DNS服务器 192.168.100.100 （可选）

MTU 1500 (如非必要，请勿改动，默认值1500)

保存 还原

MAC 地址克隆

本页设置路由器对广域网的 MAC 地址某些 ISP 可能会要求对 MAC 地址进行绑定，此时 ISP 会提供一个有效的 MAC 地址给用户，您只要根据它所提供的值，输入到“MAC 地址”栏，保存即可。 **MAC 地址**：设置路由器对广域网的 MAC 地址，当前显示的值为路由器对广域网的 MAC 地址。 **克隆 MAC 地址:**设置计算机的 MAC 地址为路由器对广域网的地址。 **恢复出厂 MAC**：把路由器对广域网的 MAC 地址的值还原到出厂默认值。	

域名服务器设置

DNS，Domain Name System 或者 Domain Name Service（域名系统或者域名服务）。执行域名服务的服务器称之为 DNS 服务器，通过 DNS 服务器来应答域名服务的查询。

域名服务设置：选择“启用”之后，域名服务器的设置开始生效，路由器的 DHCP 服务器将为请求的客户端分配添加的 DNS 域名服务器地址。

域名服务器（DNS）地址：请添加您从 ISP 获取的 DNS 域名服务器地址。

备用 DNS 地址：如果您的 ISP 提供给您两个 DNS 域名服务器地址，那么您可以把另一个 DNS 输入到“备用

<table>
<tr>
<td>DNS 地址（可选）”项中。

例如：ISP 提供给您的
<table>
<tr><td>域名服务器地址</td><td>202.96.128.166</td></tr>
<tr><td>备用 DNS 地址</td><td>202.96.134.133</td></tr>
</table>
那么您需如右图填写您的参数信息</td>
<td></td>
</tr>
</table>

第6 章：无线设置

本章主要向您介绍无线相关设置，主要包括无线基本设置，安全设置，访问控制和高级设置。

无线模式

该路由器支持两种无线工作模式：AP 模式与 Station 模式。

AP 模式：默认为 AP 模式，此模式是无线路由器最常用的工作模式，无线工作站通过搜寻 SSID 接入到无线网络中，以共享路由器的网络资源，实现资源共享等。

Station 模式：即工作站模式，选择此种模式用来连接一个 AP，以共享那个 AP 提供的网络资源，为了连接上无线网络中的 AP，需要搜寻到 AP 并提供安全论证。

SSID：SSID(服务区标识

无线模式
无线模式: AP Station
SSID:
MAC:
信道: 1
安全模式: WPA2-PSK
WPA/WPA2 算法: TKIP AES
密码:
打开扫描
保 存 还 原

符)是 AP 唯一的 ID 码。无线工作站(Station)必须出示正确的 SSID，与无线访问点 AP 的 SSID 相同，才能访问 AP。可以单击[打开扫描]按钮自动搜寻到可用的 AP 的 SSID。 **MAC：**如果要连接上 AP，还需提供该 AP 的 MAC 地址，可以通过单击[打开扫描]按钮自动搜寻到可用的 AP 的 MAC。 **信道：**可用 AP 的正在使用的信息通道，可以通过单击[打开扫描]按钮自动搜寻到可用的 AP 的信道。 **安全模式：**路由器提供以下几种安全模式认证：（1）WEP 密钥：可以选择 ASCII 码（5 或 13 个 ASCII，禁止输入/“‘等非法字符）或者 HEX（16 进制数有效字符）（10 或 26 个 16 进制数）。	

（2）WPA/WPA2-个人(PSK)。WPA 代表的含义是无线保护存取。WPA/WPA2-个人 PSK 是一种新的标准安全性技术，其中每个信息封包都以不同模式的密钥加密。由于密钥经常更改，因此 WPA/WPA2 非常安全 WPA-PSK / WPA2– PSK 使用 TKIP 或 AES 加密算法。 **WEP 模式：** Open(): Share(共享密钥):共享密钥要求接入点和终端间 WEP 密钥相同时,才允许设备加入网络. **默认密钥：**输入 WEP 密钥后,选择一个密钥作为启用的密钥,如可以选择 Key 1(即选择了 WEP 密钥 1)。 **密钥格式：**ASCII:输入 13 个字符(区分大小写),范围	

从"a-z", "A-Z"和"0-9"(例如: MyKey 12345678)。HEX（十六进制）:输入 26 个 16 进制数,范围从:"A- F","a-f" 和"0-9"(例如: 00112233445566778899AABBCC) **WEP 密钥 1：**如果[默认密钥]中选择 KEY 1，则启用该密钥。 **WEP 密钥 2：**如果[默认密钥]中选择 KEY 2，则启用该密钥。 **WEP 密钥 3：**如果[默认密钥]中选择 KEY 3，则启用该密钥。 **WEP 密钥 4：**如果[默认密钥]中选择 KEY 4，则启用该密钥。 **算法：**AES ，如果 AP 使作的是 TKIP 算法，则选择 TKIP 和 AP 服务提供者相	

对应。即该规则要对应 AP 提供者的设置。 **密码：**当选用 WPA- PSK /WPA2-PSK 认证方式时，在这里输入 AP 提供者的访问密码。 **保存：**单击"保存"按钮让您的配置生效。	

基本设置

网络模式：根据无线客户端类型选择其中一种模式。支持 11b/g/n 混合模式，11b 模式，11g 模式，11b/g 混合模式。 **主 SSID：**服务集合标识符、无线信号的网络名称，可修改，主 SSID 为必填项。 **次 SSID：**服务集合标识符、无线信号的网络名称，可修改，次 SSID 为可选项。	

广播 (SSID)：选择“关闭”禁止路由器广播 SSID，无线客户端将无法扫描到路由器的 SSID。选择“关闭”后，客户端必须知道路由器的 SSID 才能与路由器进行通讯，默认为“开启”。 **BSSID**： 是无线网络的业务组标识符，在 IEEE 802.11 中，BSSID 是无线 AP 的 MAC 地址。 **标准信道**：路由器当前使用的信道，从下拉列表中可以选择其它有效工作信道，可选项在 1-14 之间。 **扩展信道**：用于确定 11n 模式时本网络工作的频率段。 **信道带宽**：选择信道带宽以提高无线性能。当无线网络中同时有 11b/g 和 11n 客户端时，可选择宽带为 40M 的 802.11n 模式(wide)；无线网络中只有非 11n 客户端时可选择带宽为 20M 模式。	

无线安全设置

通过该页面进行无线安全方面的设置，在这里向您介绍最常用的六种加密方式(共支持十种加密方式)，其中包括 Mixed WEP 加密、WPA-个人、WPA-企业、WPA2-个人、WPA2-企业等。

1. Mixed WEP

有线等效保密（WEP）协议是对在两台设备间无线传输的数据进行加密的方式，用以防止非法用户窃听或侵入无线网络。WEP 安全技术是基于 RC4 的 RSA 数据加密技术。为无线网络通信提供数据机密性、完整性及认证功能。

选择 SSID：选择要设置的 SSID，可以对主 SSID 和次 SSID 进行不同类型的安全加密设置。

安全模式:可从列表中选择相应的安全加密模式，本路由器支持 Mixed WEP、

WPA 等多种加密模式。 **WEP 密钥**：可以设置 ASCII 码，十六进制两种格式的 WEP 密钥。 ***密钥说明：*** **可以选择ASCII码（5 或 13 个ASCII，禁止输入 / “‘等非法字符）或者 16 进制数有效字符（10 或 26 个 16 进制数）。** **默认密钥:**可以从预先设置好的 4 组密钥中选择其一个作为当前有效密钥。	

2. WPA-个人

WPA 是一种基于标准的可互操作的 WLAN 安全性增强解决方案，可大大增强现有以及未来无线局域网系统的数据保护和访问控制水平。WPA 源于正在制定中的 IEEE802.11i 标准并将与之保持前向兼容。WPA	

可保证 WLAN 用户的数据受到保护，并且只有授权的网络用户才可以访问 WLAN 网络。WPA 采用比 WEP 更强的加密算法。 **WPA 加密规则：**可以选择 AES（高级加密标准）模式、TKIP（时间密钥完整性协议）模式。 **密钥：**请输入您想使用的加密字符串，密钥字符为 8 到 63 个 ASCII 码字符。 **密钥更新周期：**为您设定的密钥生成一个有效期。	

3.WPA2-个人

WPA2(Wi-Fi Protected Access version 2)能提供比 Wireless Equivalent Privacy（WEP）或 Wi-Fi Protected Access（WPA）更佳的安全性。采用除 TKIP 加密，还提供 AES 这种新	无线安全设置 选择SSID Tenda 安全模式 -- "Tenda" 安全模式 WPA2 - 个人 WPA加密规则 TKIP AES TKIP&AES 密钥 ABCSF32F 密钥更新周期 3600 秒 保存 还原

的加密模式。 **WPA 加密规则：**可以选择 AES（高级加密标准）模式、TKIP（时间密钥完整性协议）模式，TIKIP&AES 混合模式。 **密钥：**请输入您想使用的加密字符串，注意长度和有效字符为 8 到 63 个 ASCII 码字符。 **密钥更新周期：**为您设定的密钥生成一个有效期。	

4. WPA-Enterprise

WPA-企业，此种加密是基于 RADIUS 服务器认证和 WPA 加密模型，此种加密的使用必须有一个 RADIUS 认证服务器和路由器相连接。 **Radius 服务器地址：**请输入 Radius 服务器的 IP 地址。	

Radius 服务器端口：请输入 Radius 服务器使用的认证端口。默认为 1812。 **共享密钥：**在此输入路由器对认证服务器的认证密钥，密钥字符为 8 到 63 个 ASCII 码字符。 **会话超时：** 路由器和认证服务器认证时间间隔，默认值为 3600s。	

5. WPA2-Enterprise

WPA2-企业，此种加密是基于 RADIUS 服务器认证和 WPA 加密模型，此种加密的使用必须有一个 RADIUS 认证服务器和路由器相连接。 **Radius 服务器地址：**请输入 Radius 服务器的 IP 地址。 **Radius 服务器端口：**请输入 Radius 服务器使用的认	

证端口，默认值为 1812。 **共享密钥：**在此输入路由器对认证服务器的认证密钥，密钥字符为 8 到 63 个 ASCII 码字符 **会话超时：**路由器和认证服务器认证时间间隔，默认值为 3600s。	

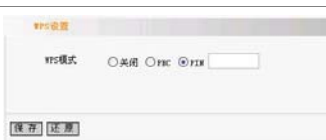
6. 802.1X

802.1x 也是基于 Radius 服务器的安全算法，路由器必须与一个有效的 Radius 服务器相连接。802.1x，是一个基于端口的认证协议，是一种常用的认证算法，端口可以是物理端口也可以是逻辑端口，如基于 VLAN 划分的端口，但对无线局域网的用户来说，意味着每一个“通道”，采用 801.11x 的最终目的是判断端口是否可用，如果认证成功，您可以	

使用此端口，允许数据流通过，否则，数据流将不允许通过，您可以开启或关闭此功能项。 **WEP**：通过选择"**开启/关闭**"来启用或关闭此加密算法。 **Radius 服务器地址**：请输入 Radius 服务器 IP 地址。 **Radius 服务器端口**：请输入 Radius 服务器使用的认证端口，默认值为 1812。 **共享密钥**：在此输入路由器对认证服务器的认证密钥，注意长度和有效字符为 8 到 63 个 ASCII 码字符。 **会话超时**：路由器和认证服务器认证时间间隔，默认值为 3600s。 ***注意：*** **为了提高安全等级，请您不要使用在字典中**	

容易检索到的单词作为密钥，有必要使用复杂强健的密钥以提高信息安全。另外在您对这十种安全模式不是很熟悉的情况下，建议您使用“WPA-个人”模式。	

WPS 设置

Wi-Fi 保护设置（WPS）能够简单、快捷地在无线网络客户端和路由器之间建立加密连接，您不必选择加密方式和密钥，只需输入 PIN 或者选择 PBC (或按路由器前面板的 WPS 按钮)来简易地设置 WPS。 **WPS 模式：**支持两种类型的简易 WPS 设置，PBC(Push-Button Configuration)和 PIN 码。	

PBC：选择 PBC 或按住路由器面板上的 WPS 按钮（**按此按钮 1 秒钟后，WPS 灯将会闪烁 2 分钟左右，表示该功能已启用，在此间隔时间内，无线客户端可以启用 WPS/PBC 进行认证协商，目前此功能只支持单一客户端，2 分钟过后，WPS 灯将熄灭。**）同时在客户端启用 WPS/PBC 进行连接。 **PIN**：如果您要使用 PIN 必须知道无线客户端的 PIN 码，添加到输入框中保存即可，同时在客户端使用相同的 PIN 码进行连接。 ***注意：*** **在使用“WPS设置”功能时，接入的客户端需支持WPS功能。**	

WDS 设置

无线分布式系统（WDS），用来扩大现有无线网络覆盖范围，该路由器支持三种模式：**Lazy、桥模(Bridge)、中继模式（Repeater）。**

Lazy：在该模式下，对端无线设备必须为 Bridge 模式或 Repeater 模式，在对端的无线设备上设置本路由器的 BSSID 即可实现无线连接。

Bridge：在该模式下，把对端 MAC 手动或通过扫描选择添加到各自 AP MAC 地址表中，点击“保存”即可实现两个有线网络的无线连接。

Repeater：在该模式下，把对端 MAC 手动或通过扫描选择添加到各自 AP MAC 地址表中，即可实现无线网

络信号的放大和扩展。 **加密类型：**支持三种加密类型，WEP、TKIP 和 AES。 **加密密钥：**输入无线设备之间的加密密钥。 **AP MAC 地址：**请输入对端无线设备的 MAC 地址。 ***注意：*** **建议两个无线设备使用相同无线信道带宽及相同的信道。**	

无线高级设置

本章节主要向您介绍无线高级功能设置，使用无线高级设置可以详细地设置无线参数，包括无线前导码，80211g/n 速率，Fragmentation 阈值，RTS 阈值等。	

BG 保护模式：有利于较慢的无线连接在复杂的多种模式下能顺利连接到路由器，默认为 Auto。 **基本数据速率：**根据实际需要，调整无线传输速率。默认值为 1-2-5.5-11Mbps。 **Beacon 间隔：**设置 Beacon 间隔参数，默认值为 100，建议不要更改默认值。 **Fragment 阈值：**每个数据包需要被分段的大小；默认值为 2346，建议不要更改默认值。 **RTS 阈值：**RTS（Request to send），当数据包的大小超过这个阈值时，使用 CTS/RTS 机制，降低发生冲突的可能性，建议不要更改默认值。 **TX 功率：**该项用来设置无	

线发射功率等级。默认值为100。 **WMM Capable**：开启时可以提高无线多媒体数据传输性能（如：视频或在线播放），如果您对 WMM 不熟悉，请设置为开启。 **APSD Capable**：自动省电模式，默认为关闭。	

无线访问控制

无线访问控制功能是以 MAC 地址为条件允许或禁止指定的客户端接入到无线网络。 **MAC 地址过滤**：开启/关闭 MAC 地址过滤功能。 **配置 MAC 地址**：请输入您要允许或禁止无线客户端的 MAC 地址。点击“添加”	

即可。 **MAC 地址列表：**显示配置添加后的 MAC 地址列表，您可以根据需要添加或删除。	

无线连接状态

本页显示无线客户端的连接信息，包括 MAC 地址信息，速度信息等。 **MAC 地址：**显示当前连接路由器的主机 MAC 地址。 **带宽：**显示当前连接主机(接入的无线客户端)使用的信道带宽。	

第 7 章： DHCP 服务设置

DHCP 服务器为您局域网中所有的计算机正确配置 TCP/IP 协议相关参数，如果您启用本路由器的 DHCP 服务器功能的话，您可以让 DHCP 服务器自动替您配置局域网中各计算机的 TCP/IP 协议（TCP/IP 协议设置包括 IP 地址、子网掩码、网关以及 DNS 服务器等），而免去手动设置 TCP/IP 相关参数。

DHCP 服务器：通过此功能开关，可以开启/关闭 DHCP 服务器自动分配 IP 地址的功能。

IP 池开始地址：DHCP 服务器所自动分配的 IP 的起始地址。

IP 池结束地址：DHCP 服务器所自动分配的 IP 的结束

DHCP服务设置

DHCP服务器	✓ 启用
IP池开始地址	192.168.0. 100
IP池结束地址	192.168.0. 200
过期时间	一天

保存 还原

地址。 **过期时间：**设置 DHCP 服务器分配 IP 地址的租用时间，设置合适的租用时间,可提高 DHCP 服务器对作废 IP 地址的回收效率。 例如：设置租约时间为一个小时,那么 DHCP 服务器将每一个小时回收一次作废的 IP 地址。	

DHCP 客户端列表

DHCP 客户端列表可以显示客户机从路由器 DHCP 服务器获取的 IP 地址，MAC 地址，主机等信息。您可以手动输入 IP 和 MAC 地址，将它转换为静态分配。根据接入的计算机的 MAC 地址，路由器查找列表中相关表项,分配相应 IP 地址，如果不能在列表中找	

到对应计算机静态绑定项，则从 DHCP 池中分配未分配的 IP 地址给该计算机。 **IP 地址**：请输入需要静态绑定的 IP 地址。 **MAC 地址**：请输入需要绑定的计算机的 MAC 地址。 **Hostname**：显示绑定的计算机的主机名。 **Lease**：显示当前列表项租约期所剩余的时间。	

第 8 章： 虚拟服务器

单端口映射

单端口映射定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过 IP 地址指定的局域网网络服务器。单端口映射允许建立各种公共服务，例如 WEB 服务器、FTP 服务器等。

外网端口：WAN 端服务端口，即提供外网服务的端口;

内网端口：LAN 端服务端口，即客户端 PC 的端口；

内网 IP：局域网中作为服务器的计算机的 IP 地址；

协议：包含 TCP、UDP 和全部。

启用：只有选中该项后本条

目所设置的规则才能生效。 **删除：**清空该项的所有设置参数。 在“**常用服务端口**”中，列出了常用的协议的端口，您可以在其中选中一个，然后在 ID 中选一个序列号，然后单击“填充到”，将这个端口自动添加到列表中，对于常用服务端口中没有列出的端口，您也可以手动添加。 **填充到：**帮助您把常用的服务端口写到您要设置的一项。 例如，局域网中 IP 地址为 192.168.0.10 的服务器提供端口为 80 的 WEB 服务，如需 Internet 上的客户访问到此服务器的 40 端口，则需如右图设置。 ***注意：*** **如果设置了服务端口为 80 的虚拟服务器，则需要**	

将“安全设置”菜单中“远端WEB管理”项设置为 80 以外的值，如 8080，否则会发生冲突，而导致虚拟服务器不可用。

端口段映射

端口段映射定义了广域网服务端口范围的访问和局域网网络服务器之间的映射关系，所有对该广域网服务端口段范围内的访问，将会被重定位给通过 IP 地址指定的局域网网络服务器。

开始端口~结束端口：映射的内网主机提供的服务端口段。

内网 IP：局域网中作为服务器的计算机的 IP 地址。

协议：包含 TCP、UDP 和

全部。 **启用**：只有选中该项后本条目所设置的规则才能生效。 **删除**：清空该项的所有设置参数在“**常用服务端口**”中，列出了常用的协议的端口，您可以在其中选中一个，然后在 ID 中选一个序列号，然后单击“填充到”，将这个端口自动添加到列表中，对于常用服务端口中没有列出的端口，您也可以手动添加。 **填充到**：帮助您把常用的服务端口写到您要设置的一项。 例如：局域网中 IP 地址为 192.68.0.10 的服务器提供端口为 80 的 WEB 服务和 23 端口的 Telnet 服务，如需 Internet 上的客户访问到此服务器，则需如右图所示的设置。	

注意： 如果设置的端口端口中包括了服务端口为 80 的虚拟服务器，则需要将“安全设置”菜单中“远端WEB管理”项设置为 80 以外的值，如 8080，否则会发生冲突，而导致虚拟服务器无效。	

端口触发

内网客户端访问因特网上服务器，对于某些应用，客户端向服务器主动发起连接的同时，也需要服务器向客户端主动发起连接请求，而缺省情况下路由器收到 WAN 口主动连接的请求都会拒绝，这样就会中断通信。通过定义**端口触发**规则，当客户端访问服务器触发此规则后，路由器自动开放服务器需要向客户端请	

求的端口，这样可以保证通信正常。 **IP 地址范围：**该应用客户端主动向外部服务器发起请求的 IP 范围。即只有这范围的 IP 才能使用此规则。 **触发端口：**该应用客户端主动向外部服务器发起请求的端口范围。取值范围：1～65535，端口范围必须从小到大。如果只有一个端口，则两处填写同一端口号。 **传入端口：**允许外部服务器主动向客户端发起请求的端口范围。取值范围：1～65535，该应用客户端主动向外部服务器发起请求的端口范围。取值范围：1～65535，端口范围必须从小到大。如果只有一个端口，则两处填写同一端口号。 **启用：**使能或禁用本规则。	

添加至列表：编辑完成后，点击<添加到列表>按钮可以把当前编辑的规则添加到端口触发表中。 **保存：**用户单击“保存”后，当前所编辑的规则才能生效。 **还原：**用户单击“还原”后，放弃上一次“保存”之后的所有操作。 允许在表中对先前配置的规则进行删除、修改等操作。 ***注意：*** **每个定义的特殊应用只能同时被一台PC所使用。如果有多台机器同时打开一个“触发端口”，那么“外来端口”的连接只会被重定向到最后一次打开“触发端口”的那台PC。**	

ALG 应用

ALG(Application Layer Gateway)即应用层网关一些早期设计的应用层协议，比如 FTP、TFTP，在穿越 NAT 设备后往往不能正常工作。在这种情况下，您可以在本页面启用相应协议的 ALG，来克服这些问题。FTP、TFTP 这些应用层协议，客户端会先通过某个知名端口连接到服务器，进行控制交互。在这个过程中，客户端的报文里通常会携带有自己机器本身的 IP 地址和端口号，告知服务器后续数据发往报文里的指定的 IP 地址和端口号。如果客户端是经过 NAT 设备接入 Internet 的话，那么服务器将无法直接访问到客户端指定的地址和端口。ALG 正是为了解决这个问题而设计的，它可以将报文里客



户端的 IP 地址和端口改成 NAT 设备的 IP 地址和一个空闲的端口号，后续服务器发往 NAT 设备的数据将会被正确地转发到内网的客户端。 路由器缺省情况下，以下协议的 ALG 已经启用，**建议保留缺省设置，不做修改**。 1、FTP 2、TFTP 3、PPTP 4、IPSec 5、L2TP	

DMZ 主机

在某些特殊情况下，我们需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可把该计算机设置为 **DMZ 主机**。 **DMZ 主机 IP 地址：**请在	DMZ主机 注意：设置DMZ主机之后，与该IP相关的防火墙设置将不起作用。 DMZ主机IP地址 192.168.0.10 启用 保存 还原

DMZ 主机 IP 地址栏内输入欲设为 DMZ 主机的局域网计算机的 IP 地址。 **启用**：点击实现 DMZ 主机的开启和关闭功能。 例如:把局域网中 IP 地址为 192.168.0.10 的计算机设置为 DMZ 主机，以实现它与 Inter net 上另一台主机双向通信,则需如右图设置。 ***警告:*** **当把主机设置成DMZ主机后，该计算机完全暴露于外网，防火墙对该主机不再起作用。**	

UPnP 设置

UPnP (通用即插即用网络协议)，此功能需要 WindowsXP/WindowsME 操作系统(注：系统需集成	

或已安装 Directx 9.0)或支持 UPnP 的应用软件才能生效。依靠 UPnP 协议，局域网中的主机可以请求路由器进行特定的端口转换，使得外部主机能够在需要时访问内部主机上的资源。 **启用 UPnP**：选择实现 UPNP 的开启和关闭功能。	

第 9 章：宽带控制

宽带控制可以限制内网计算机上网的通信流量，设备可以最多设置 20 条限制规则，最多同时支持 254 台 PC 的流量限制，并支持地址段的配置方式。

启用带宽控制：开启和关闭内网 IP 带宽控制功能。

接口：限制 WAN 口的上传带宽和下载带宽。

服务：选择受限制的服务类型。比如 HTTP 服务。

IP 起始地址：需要流量控制的主机 IP 地址范围内的第一个。

IP 结束地址：需要流量控制的主机 IP 地址范围内的最后一个。

限速方向:对该 IP 地址范围内每 IP 应用的限速方向,可

选择只限上传方向、下载。 **带宽范围:**允许指定 IP 范围内的主机上传/下载的最小到最大数据流量,单位是 KB/s。上传/下载的上限不得超过 WAN 口的上限范围。 **启用:** 启用当前编辑的规则。如果没选，虽然存在这条规则，但不启用。 **添加到列表:** 编辑完成后，点击"添加到列表"按钮可以把当前编辑的带宽控制规则加入规则表中。 **保存:**用户单击"保存"后，当前所编辑的规则才能生效。 **还原:** 用户单击"还原"后，放弃上一次"保存"之后的所有操作。 允许在表中对先前配置的规则进行删除、修改等操作。	

第10章： 安全设置

客户端过滤

为方便您对局域网中的计算机进行进一步管理，您可以通过数据包过滤功能来控制局域网中计算机对互联网上某些端口的访问。

客户端过滤：启动“客户端过滤”。

请选择：如果您已经配置好过滤要求，请直接选择配置文件。

启用:开启/关闭此过滤规则。

过滤模式:选择“禁止”选项，则禁止规则中 IP 地址的主机对应的端口通过路由器；选择“允许”选项，则允许规则中 IP 地址的主机对应的端口通过路由器。

注释：即为此配置文件定义

的简单描述。 **IP**：填入局域网中被控制的计算机的 IP 地址，您可以使用一个 IP 地址范围。 **端口**：添写预控制的 TCP/UDP 协议端口，您可以指定一个端口范围。 **类型**：选择被控制的数据包所使用的协议（“ALL”包括 TCP/ UDP）。 **时间**：填入本条规则生效的起始时间和终止时间； **日期**：根据自身的要求选择相应的选项。 例如：如果您希望局域网中 IP 地址为 192.168.0.10 的计算机在每周的 8：00-18：00 时间段内不能浏览 WEB 网站，对局域网中其它计算机则不做任何限制，这时您需要指定如右图的数据包过滤表。	

URL 过滤

为方便您对局域网中的计算机所能访问的网站进行控制，您可以使用域名过滤功能来指定在什么时段不能访问哪些网站。

URL 过滤功能：启动“DNS 过滤功能”。

请选择：假如您已经配置好过滤要求，请直接选择配置文件。

启用：开启/关闭此过滤规则。

过滤模式：选择“禁止”选项，则禁止规则中 IP 地址的主机对应的数据包通过路由器；选择“允许”选项，则仅允许规则中 IP 地址的主机对应的数据包通过路由器。

注释：即为此配置文件定义的简单描述。

IP：填入局域网中被控制的计算机的 IP 地址，您可以使用一个 IP 地址范围。 **URL 字符串**：填入被过滤的域名和域名的一部分。 **时间**：填入希望本条规则生效的起始时间和终止时间。 **日期**：根据自身的要求选择相应的选项。 **保存**：完成使设置生效。 例如：如果您希望局域网中 IP 地址为 192.168.0.11 的计算机不能浏览包含“sex”字符串的 WEB 网站，这时，您需要指定如右图的数据包过滤表。	

MAC 地址过滤

为了更好的对局域网中的计算机进行管理，您可以通过 MAC 地址过滤功能	

控制局域网中计算机对 Internet 的访问。

MAC 地址过滤:选择“启用”开启 MAC 地址过滤功能。

请选择：如果您已经配置好过滤规则，请直接选择配置文件。

启用:开启/关闭此过滤规则。

过滤模式：选择“禁止”选项，则禁止规则中 MAC 地址的主机通过路由器；选择“允许”选项，则仅允许规则中 MAC 地址的主机通过路由器。

注释：即为此配置文件定义的简单描述。

MAC 地址：把计算机的 MAC 地址添加进 MAC 地址栏里。

时间：填入您希望本条规则生效的起始时间和终止时间。 **日期**：根据自身的要求选择相应的选项。 **保存**：完成使设置生效。 例如：如果您希望局域网中 MAC 地址为 00:C0:9F:AD:FF:C5 的计算机在 8：00-18：00 时间段内不能访问 Internet，而希望局域网中的其它计算机能访问 Internet，这时您需要指定如右图的数据包过滤表。	

防网络攻击

启用防网络攻击功能，当开启该功能后，路由器将启动防网络攻击功能。当监测到有主机向路由器发起攻击时，将自动限制其带宽。您可以单击“系统工具”里的系	

统日志选项查看发起攻击主机的 IP 地址。 **防网络攻击：**选择“启用”开启防网络攻击功能。	

远端 WEB 管理

本节设置路由器在广域网中可以执行远端 WEB 管理的计算机的 IP 地址和 WEB 管理端口； **启用：**开启远端 WEB 管理功能； **端口：**可以执行远端 WEB 管理的端口号； **WAN 口地址段：**输入广域网中可执行远端 WEB 管理的 IP 地址段 ***注意：*** **1、如果您想通过 8080 端口登录路由器，则您**	

必须用“IP地址（此IP地址为路由器WAN口IP地址）：端口”的方式（例如http：//192.168.1.2:8080）才能登录路由器执行WEB界面管理； 2、假如您的WAN口地址的起始和终止IP均为 0.0.0.0，则在此状态下，广域网中所有计算机都能登录路由器执行远端WEB管理；如果您改变了WAN口地址段为218.88.93.33-218.88.93.35 则广域网中只有此IP地址段中的IP（例如 218.88.93.33、218.88.93.34 和218.88.93.35）的计算机才能登录路由器执行远端WEB管理。 例如，我们仅允许Internet上拥有IP地址	

为 218.88.93.33 的计算机通过 80 端口访问到此管理界面，那么需如右图填写您的参数信息。	

本地 WEB 管理

本地 WEB 管理可以实现在局域网中，授权指定的 PC 登录 Web 进行管理。 **启用**：开启本地 WEB 管理功能。 **MAC 地址**：可以执行本地 WEB 管理的计算机的 MAC 地址。 ***注意：*** **1、在默认状态下，此功能不启用，则本地PC均可登录Web进行管理。** **2、例如，我们仅允许**	

本地MAC地址为 00:11:22: 33:E4:F 5 的计算机可以进行 Web管理，那么需如右图填写您的参数信息。 3、如果仅设置“启用”此功能而不添加访问的MAC地址，那么会导致所有的计算机都不能通过WEB访问路由器的管理界面。	

WAN 口 Ping

当开启该功能后，广域网的计算机将不能 Ping 到本路由器(即路由器不会响应来自 Ping 请求)，内网的计算机才可以 ping 通。 **忽略来自 WAN 口 Ping:** 启用此功能后路由器将不再回应来自 WAN 口的 Ping 检测。	

第 11 章：　路由设置

本章节主要向您介绍路由表的概念，及怎样设置静态路由。

路由表

本页显示本路由器的核心路由表。

★小知识：路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表，供路由选择时使用。

路由表

目的IP	子网掩码	网关	跳跃数	接口
192.168.100.0	255.255.255.0	0.0.0.0	0	eth2.2
192.168.0.0	255.255.255.0	0.0.0.0	0	br0
0.0.0.0	0.0.0.0	192.168.100.100	0	eth2.2

刷新

静态路由

<table>
<tr>
<td>
本页用来设置路由器的静态路由功能。

目的网络 IP：欲访问的主机的 IP 地址或 IP 网段。

子网掩码：填入子网掩码，一般为 255.255.255.0。

网关：数据包被发往的路由器或主机的 IP 地址。

★小知识：由系统管理员事先设置好固定的路由表称之为静态（static）路由表，一般是在系统安装时就根据网络的配置情况预先设定的，它不会随未来网络结构的改变而改变。

注意：
<u>1、网关IP必须是与本路由器LAN口属于同</u>
</td>
<td>
目的网络IP　子网掩码　网关　操作
添加
</td>
</tr>
</table>

一个网段。 2、目的IP地址如果是一台主机IP地址，子网掩码须为 255.255.255.255。 3、目的IP地址如果为IP网段，则须与子网掩码匹配。例如，如果目的IP为 10.0.0.0，子网掩码须为 255.0.0.0；如果目的IP为 10.1.2.0，子网掩码须为 255.255.255.0。	

第 12 章：系统工具

时间设置

本节设置路由器的系统时间，您可以选择自己设置时间或者从互联网上获取标准的 GMT 时间。 **时区：** 选择您所在时区。 **自定义时间：** 输入您需要设置的时间。 ***注意：*** **关闭路由器电源后，时间信息会丢失，当您下次开机连上Internet后，路由器将会自动获取GMT时间。您必须先连上Internet获取GMT时间或到此页设置时间后，其他功能（如防火墙）中的时间限定才能生效。**	时间设置 时区： （GMT+08:00）北京，重庆，乌鲁木齐，香港特别行政区，台北 （注意：仅在连上互联网后才能获取GMT时间。） 自定义时间： 2008 年 02 月 16 日 18 时 06 分 01 秒 保 存 还 原

动态 DNS

DDNS（Dynamic Domain Name Server）是动态域名服务的缩写。DDNS 是将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析。

其主要作用是：

1、宽带营运商大多只提供动态的 IP 地址，DDNS 可以捕获用户每次变化的 IP 地址，然后将其与域名相对应，这样其他上网用户就可以通过域名来与用户交流了。

2、DDNS 可以帮你在自己的公司或家里构建虚拟主机。

<table>
<tr>
<td>
服务提供商：选择您使用的 DDNS 服务提供商。

用户名：请您输入在 DDNS 服务供应商上注册的用户名。

密码：请您输入在 DDNS 服务供应商上注册的密码。

域名：输入注册有效的域名（可选）。
例如：在本地 192.168.0.10 主机上建立一个 WEB 服务器，并在花生壳注册如下：
<table>
<tr><td>用户名</td><td>tenda</td></tr>
<tr><td>密码</td><td>123456</td></tr>
<tr><td>域名</td><td>test.vicp.net</td></tr>
</table>
在虚拟服务中映射好端口(请参考第 8 章)，在 DDNS 服务中设置账户信息后，在浏览器的地址栏中输入“http：//test.vicp.net” 就可以访问你的 WEB 页了。
</td>
<td></td>
</tr>
</table>

备份/恢复设置

在这里您可以备份当前或恢复以前的路由器设置。	
备份设置：点击“**备份**”按钮，即可导出配置文件，再选择保存路径。 点击“**保存**”即可保存配置文件。	
恢复设置：点击“**浏览**”按钮，选择之前备份的配置文件。 点击“**恢复**”按钮即可恢复到以前的配置。	

软件升级

通过升级本路由器的软件，您将获得更加稳定的路由器版本及增值的路由功能。 您可从 www.tenda.com.cn 上获	

<table>
<tr><td>得路由器升级文件。

浏览：点击“浏览”按钮，选择升级文件。

升级：点击“升级”按钮，开始升级过程，升级完成后，路由器自动重启。</td><td>软件升级
请通过升级本路由器的软件，您将获得新的功能。
选择固件文件:
浏览... 升级
当前系统版本: 1.0.73; 发布日期:2008-02-15
注意：升级过程不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级成功后，路由器将自动重启。升级过程约数分钟，请等候。</td></tr>
</table>

恢复出厂设置

<table>
<tr><td>单击“恢复出厂设置”按钮将使路由器的所有设置恢复到出厂时的默认状态。
默认出厂设置
登陆用户名： admin
登录密码： admin
IP 地址： 192.168.0.1
子网掩码： 255.255.255.0

注意:
<u>恢复出厂设置后，需重新启动路由器才能生效。</u></td><td>恢复出厂设置
单击此按钮将使路由器的所有设置恢复到出厂时的默认状态。
恢复出厂设置</td></tr>
</table>

重启路由器

本节重启路由器，重启路由器将使设置在改变后生效。路由器在重启后，会自动断掉 WAN 口连接。

重启路由器： 点击重启路由器。

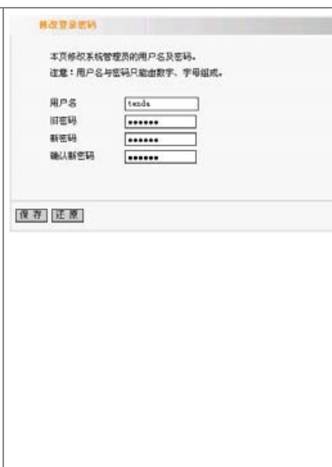


修改登录口令

修改系统管理员的登录口令。

请您首先输入原来的登录口令，然后输入您希望使用的新登录口令，如果您原来的登录口令输入无误的话，单击“保存”即可成功修改用户登录口令。

例如，我们将用户名及密码修改为：



用户名	tenda
密码	tenda

那么需如右图填写您的参数信息。

注意：

出于安全考虑，我们强烈推荐改变初始用户名及密码。

系统日志

在系统日志里，您可以查看系统启动后出现的各种情况，也可以查看有无网络攻击发生。系统日志的最多记录不超过 150 条。



刷新：刷新当前系统日志。

清除日志：清除所有日志记录。

附录 ：

- 路由器、四口千兆交换机、无线接入点、防火墙四位一体
- 符合 IEEE802.11n（draft 2.0）标准，向下兼容 IEEE802.11b、IEEE802.11g
- 利用 MIMO 技术和信号反射原理使其传输距离在 802.11g 的标准上增加了 8 倍，并有效减少覆盖区域内的盲点
- 提供 300Mbps 的接收速率与 300Mbps 的发送速率
- 支持 WMM，让您的语音、视频更流畅
- 支持 64/128 位 WEP、WPA、WPA2、802.1x 安全机制
- 支持“一键加密”功能
- 方便快捷的配置向导，使您无需进入路由器的管理界面，即可设置路由与 Internet 的连接
- 支持远程/本地 Web 管理，全中文配置界面
- 使用无线漫游（Roaming）技术，保证高效的无线连接
- 支持隐藏无线 SSID 功能和基于 MAC 地址的访问控制
- 支持端口自动识别交叉/直通（Auto MDI/MDIX）
- 提供系统安全日志，可以记录路由器使用状态
- 支持 MAC 地址过滤，NAT 转发规则
- 支持通用即插即用（UPnP）、DDNS 功能
- 支持 30 组无线网卡 MAC 地址的授权访问
- 支持简单网络时间协议（SNTP）
- 支持虚拟服务器，DMZ 主机
- 支持 DHCP 服务器/客户端
- 内置防火墙，防黑客攻击
- 支持无线通道的自动选择
- 支持 WDS 功能（无线分布式系统）